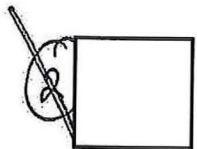




DEFENSE CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS
400 ARMY-NAVY DRIVE, SUITE 901E
ARLINGTON, VIRGINIA 22202-2884



FACSIMILE TRANSMISSION COVER SHEET
FACSIMILE TELEPHONE (703) 604-8998

DATE: 18 JUN 98

TO:

b3 Per FBI
b6 Per FBI
b7C Per FBI
b7E Per FBI

NUMBER OF PAGES: 3

Per DoW OIG (b)(6) (b)(7)(C)

FROM:

(703) 604-86

MESSAGE:

JUN 22 1998

Date: Thu, 18 Jun 1998 10:12 -0600
From: Per DoW OIG (b)(6) (b)(7)(C)
To: Per DoW OIG (b)(6) (b)(7)(C)
Subject: FW: DISN hacks

Lick your chops again...

> -----Original Message-----

> From: Per DoW OIG (b)(6) (b)(7)(C) [SMTP: Per DoW OIG (b)(6) (b)(7)(C)]
> Sent: Thursday, June 18, 1998 3:12 AM
> To: Per DoW OIG (b)(6) (b)(7)(C)
> Subject: DISN hacks

> Let me begin by stating that I am in no way affiliated with and
> so-called "hacker" group.

> About two months ago the company I was working for was involved in
> several attempted attacks on our network. Whoever was making the attempt
> was coming at us in a direction that I had never seen before. In order
> to better understand Internet attacks I turned to #hackphreak on the
> undernet from which somebody directed me to #rhino9. In rhino9 I queried
> several people on what the possible means of attacks could cause the
> symptoms I was seeing. I spent several nights chatting on rhino9 with
> two individuals that were very open to teach me their tactics for
> network intrusion. These talks eventually led to being invited to a 2600
> meeting where they felt I could better understand the methods currently
> being used by the so called "hackers". After the meeting I was invited
> back to a members house where he agreed to perform a security scan on my
> network for back doors that were vulnerable. I was hesitant at first and
> felt like I was being more or less recruited in to their so-called
> society but at the same time I was learning things that \$2000 security
> conferences hadn't taught me. After this day I only kept in contact with
> him via the undernet until last weekend.

> I had some questions on Unix security for a consulting job I
> received (I am an NT admin and Unix was beyond me) and he invited me up
> to his house to go over some basics with me. Upon arrival I began
> discussing his background and what he planned to do professionally with
> his skills. This led to information that I wish had not been discussed
> and ultimately this email. He admitted and had physical proof of the
> infamous DISN hacks. I saw network topologies, logins, passwords, host
> files, an entire binder of information of stolen documentation. I knew
> at this point that I wasn't dealing with a seventeen year old kid but in
> my eyes a threat to the country. The worst part was that he still had a
> backdoor into the network and openly showed it to me.

> Per DoW OIG (b)(6) (b)(7)(C) I am not sending you this email because I want money or
> credit for taking these guys down. I would like to remain entirely
> anonymous. This individual has a backdoor into your network and has been
> contracted by somebody out of the country (he wouldn't tell me who) to
> break into you network and obtain data. He was paid a substantial cash
> advancement and upon delivery will be paid more than you or I make in a
> year. I will help you in any way I can. I know the two individuals (it
> was only two) those hacked, and continue to hack your network. I don't
> know if you saw the CBS special a couple of weeks ago on hackers but CBS
> unknowingly interviewed the actual individuals that performed this hack.
> This is a huge joke in the underground scene. They called themselves
> "Solar" and "Sniper", these are not their real nick names. I know where
> these guys live and know for a fact that you can find physical proof of
> the hacks at their house. I was reluctant to email you but I was talking
> with some friends tonight and they had me concerned that if I didn't say
> anything that I would be a so-called "accomplice". Please let me know

> what I can do to help.

> Per DoW OIG (b)(6)
> (b)(7)(C)

> Get Your Private, Free Email at <http://www.hotmail.com>

FAX

Defense Criminal Investigative Service

* DCIS *

U.S. Department of Defense
Office of Inspector General



DEFENSE INFORMATION INFRASTRUCTURE
INTRUSION INVESTIGATIONS TEAM

DI4T

b3 Per FBI
b6 Per FBI
b7C Per FBI
b7E Per FBI

TO:
Name

Voice

Fax

DATE:

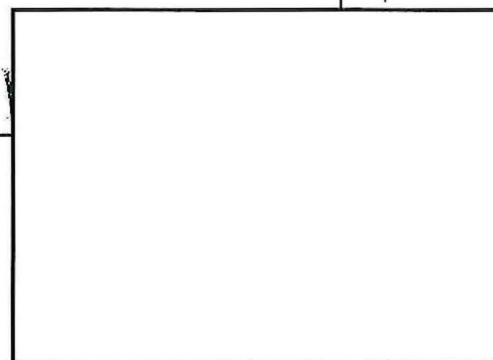
FROM: Per DoW OIG (b)(6) (b)(7) (C)
Name

Voice Per DoW OIG (b)(6) (b)(7) (C)

Fax

COVER +

COMMENTS...





(Investigations)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

9810437A-27-APR-98-00HQ-J6P

June 28, 1998

ALLEGED INTRUSION INTO DEFENSE INFORMATION SYSTEMS NETWORK (DISN)

INTERVIEW OF Per DoW : On June 21, 1998, Per DoW OIG (b) met with Special Agent Per DoW OIG (b) of the Defense Criminal Investigative Service (DCIS), Special Agent Per DoW OIG (b) of the Federal Bureau of Investigation (FBI) New York Field Office, and Per DoW OIG (b). During the conversation the Special Agents asked questions of the source relating to his knowledge of unauthorized intrusions into Department of Defense computers.

Source stated between January 1998 and June 13, 1998 he met with a person by the handle of Per DoW OIG (b)(6) (b)(7) residence located south of Irvine, California. He stated he initially met Per DoW OIG (b)(6) (b)(7) online on the Internet in the "rhino 9" chat room. Rhino 9, he explained is a group of computer users who talk about computer network vulnerabilities. He had a number of conversations with Per DoW OIG (b)(6) (b)(7) and later talked with Per DoW OIG (b)(6) (b)(7) and the source usually talked about network security and computer hacking topics. Source stated Per DoW OIG (b)(6) (b)(7) appeared to be "hacker" types who could possibly help him understand more about network security. Source recalled Per DoW OIG (b)(6) (b)(7) also went by the handle of Per DoW OIG (b)(6). Source stated both Per DoW OIG (b)(6) (b)(7) were approximately Per DoW OIG (b)(6) years old.

After some initial discussions with Per DoW OIG (b)(6) (b)(7) online, source went to Per DoW OIG (b)(6) (b)(7) and met with Per DoW OIG (b)(6) (b)(7) in January, 1998. He explained to get to the residence he drove from Per DoW OIG (b)(6) (b)(7) (C).

In this first meeting in January, 1998 source stated Per DoW OIG (b)(6) (b)(7) took him into his garage where his computer was located. Source stated he was shown documents and books in a box next to source's computer which were taken from dumpster diving at businesses. Dumpster diving, source explained, is something hackers or unauthorized network users sometimes do to collect computer reference materials as well as logon password information needed to gain unauthorized access to networks. There were also blue prints of some buildings in the box. Some of these documents were from Pacific Bell and Lucent Technologies. Using Per DoW OIG (b)(6) (b)(7) computer Per DoW OIG (b)(6) (b)(7) showed source a database of encrypted reference materials which detailed network vulnerabilities of various computer networks. He stated the items were encrypted with Blowfish software. The encryption software used a 5 digit password he stated. During this meeting Per DoW OIG (b)(6) (b)(7) showed him how to compromise computer networks using the stat-d vulnerability. Source stated the stat-d vulnerability was popular back then when compromising various computers which used the Solaris Operating System.

CLASSIFICATION:

WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the

9810437A-27-APR-98-00HQ-J6P

2

Several weeks after meeting with him, [Per DoW OIG (b)(6) (b)(7)(C)] but source continued to talk with him on the IRC in the rhino 9 chat room. They talked intermittently until source and a friend met with them on three additional occasions between April and June 13, 1998. Source stated during a meeting in April, 1998 [Per DoW OIG (b)(6) (b)(7)(C)] showed source a hacker program he had written known as OGRE. OGRE is a hacker suite which would allow a user to look at vulnerabilities of computer networks. [Per DoW OIG (b)(6) (b)(7)(C)] stated once he had finished the program he would release the final version. During this meeting source noticed [Per DoW OIG (b)(6) (b)(7)(C)] computer was scanning networks for some type of vulnerabilities. He remembered various IP addresses were coming up on the screen every couple of seconds.

In a May 1998 meeting at [Per DoW OIG (b)(6) (b)(7)(C)] home source recalled there being multiple computers in the garage at that time. He stated [Per DoW OIG (b)(6) (b)(7)(C)] had a black laptop he used and [Per DoW OIG (b)(6) (b)(7)(C)] had a computer which was connected to another computer via a Wingate modem. They had a Cable Modem connection. He stated the computer with the Wingate belonged to [Per DoW OIG (b)(6) (b)(7)(C)]. Source also remembered [Per DoW OIG (b)(6) (b)(7)(C)] used his computer to go to a site source recognized as www.hacked.net. This web site showed images of various web pages that were changed or hacked by various hackers. [Per DoW OIG (b)(6) (b)(7)(C)] showed source several web sites he had hacked himself. Source did not recall the names of these sites. Source explained that [Per DoW OIG (b)(6) (b)(7)(C)] talked about how [Per DoW OIG (b)(6) (b)(7)(C)] rode around in [Per DoW OIG (b)(6) (b)(7)(C)] van and used a cellular phone and their computer to hack into computer networks. They did the hacking this way because they were less likely to get caught being mobile and using a cellular phone. At this meeting [Per DoW OIG (b)(6) (b)(7)(C)] showed source computer programs relating to a number of Internet shell accounts and explained that he used these shell accounts to conceal his identity when he gained access to computer networks. Source saw references to these shell accounts when [Per DoW OIG (b)(6) (b)(7)(C)] was working on his computer. They were located in a CRT telnet (communications) utility program. Source also recalled seeing a stack of papers on the printer in the garage which contained many credit card numbers, with corresponding names, addresses and telephone numbers. There were about 2 credit card accounts with identifying information per page and the stack was about 2.5 inches thick. Also, [Per DoW OIG (b)(6) (b)(7)(C)] showed source a CBS video tape of an interview of two members of a hacker group known as, the Masters of Downloading (MOD). [Per DoW OIG (b)(6) (b)(7)(C)] stated they were the two MOD members who were interviewed as displayed in the video tape. [Per DoW OIG (b)(6) (b)(7)(C)] also showed source articles on a web page known as Antionline located at www.antionline.com which discussed the activities of the MOD. At this site there were multiple articles discussing the MOD's attack of Department of Defense systems and the stealing of the DEM software. Source noted that [Per DoW OIG (b)(6) (b)(7)(C)] knew [Per DoW OIG (b)(6) (b)(7)(C)], whom he also knew as [Per DoW OIG (b)(6) (b)(7)(C)].

During the May 1998 meeting [Per DoW OIG (b)(6) (b)(7)(C)] and source also hacked a web site known as www.betthenet.com. Betthenet is a web site for gambling via the Internet. It is located in the Dominican Republic. Source recalled placing an image over the existing Betthenet image that was stored on this web site.

On June 13, 1998, source met with [Per DoW OIG (b)(6) (b)(7)(C)] at [Per DoW OIG (b)(6) (b)(7)(C)] home. Source stated he saw the computers located in the garage again as he had noticed previously. He remembered seeing [Per DoW OIG (b)(6) (b)(7)(C)] computer. [Per DoW OIG (b)(6) (b)(7)(C)] He also recalled seeing the dumpster diving material in the box. At the house source stated [Per DoW OIG (b)(6) (b)(7)(C)] said he had sold some type of Department of Defense "DEM" software to some foreign guy in the Mafia. He remembered him mentioning this when he first arrived at the residence. After leaving the [Per DoW OIG (b)(6) (b)(7)(C)]

9810437A-27-APR-98-00HQ-J6P

3

home and going to a Sizzler Steakhouse restaurant source stated [Per DoW] opened his wallet and showed him money he got as a payment for the DEM software he was selling to the foreigner. He estimated it was between \$800 and \$1000. [Per DoW] stated the money was mailed to him. [Per DoW] said the software was some type of Department of Defense interface software. He said the software has to work in conjunction with security cards for it to function. He said he would sell it even without the security cards. [Per DoW] indicated he was still dealing with the guy via the Internet. After returning to the home of [Per DoW] they watched a portion of what they thought was another interview by CBS officials with [Per DoW] (b)(6) (b)(7)(C). It appeared to be some of the same video they had already seen so they turned it off. That same night of the visit [Per DoW] was revising a program known as "Bitchslap" which is a "denial of service" hacker program. He was writing the revisions in the Visual Basic programming language. This program was some type of "ping flood" program which would intentionally degrade the capability of a computer network.

Prepared by SA [] Arlington, Va, DI4T

[] b6 Per FBI
b7C Per FBI

TOTAL P.04

FAX

Defense Criminal Investigative Service

* DCIS *

U.S. Department of Defense
Office of Inspector General



DEFENSE INFORMATION INFRASTRUCTURE
INTRUSION INVESTIGATIONS TEAM

DI4T

b3 Per FBI
b6 Per FBI
b7C Per FBI
b7E Per FBI

TO:

Name _____

Voice _____

Fax _____

DATE: 29 JUL 98

FROM:

Per DoW OIG (b)(6) (b)(7)(C)

Name _____

Voice _____

Fax _____

COVER + _____

COMMENTS...



**DEPARTMENT OF DEFENSE INSPECTOR GENERAL
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
WESTERN FIELD OFFICE
26722 PLAZA ST., SUITE 130
MISSION VIEJO, CA 92691-6300**

9810437A-27-APR-98-00HQ-WOP

June 30, 1998

ALLEGED MOD INTRUSION INTO DISN

INTERVIEW OF Per DoW OIG (b)(6) : On June 29, 1998, DCIS SA's Per DoW OIG (b) and Per DoW OIG (b)(6) interviewed Per [redacted] at his residence located at Per DoW OIG (b)(6) (b)(7)(C). Also at the interview, was Per DoW OIG (b)(6) (b)(7)(C) Per DoW OIG (b)(6) (b)(7)(C) and Per DoW OIG (b)(6) (b)(7)(C). Per [redacted] consented to having Per [redacted] interviewed voluntarily by reporting agents. The purpose of the interview was to determine if Per [redacted] was involved in various DOD unauthorized computer intrusions either by himself or in concert with others. Per DoW OIG (b)(6) (b)(7)(C) requested that Per [redacted] answer our questions and then requested that Per [redacted] remain and be present for the interview. Per [redacted] advised that Per DoW OIG (b)(6) (b)(7)(C) The interview commenced at approximately 4:45 PM and ended at approximately 7:50 PM. Per [redacted] provided substantially as follows:

Per [redacted] was advised that this interview was voluntary and that his cooperation was desired. Per [redacted] advised that he had just returned last week from staying with Per DoW OIG (b)(6) (b)(7)(C) Per DoW OIG (b)(6) (b)(7)(C). Per [redacted] advised that he had only known Per [redacted] for about 1 and 1/2 months. Per DoW OIG (b)(6) (b)(7)(C) interjected that he had known him longer, possibly from January or February 1998. Per [redacted] advised that he had met Per [redacted] during discussions over the Internet in Phrack. During his stay at Per DoW OIG (b)(6) (b)(7)(C) was teaching Per [redacted] how to program in Visual Basic (VB). Per [redacted] claimed that he does not know how to program in C. They spent a lot of time on the computers in Per DoW OIG (b)(6) (b)(7)(C) garage. Per [redacted] explained that he had been going on Internet Relay Chat (IRC) for the last three years and specifically talking with hackers for about the last two years over the Internet. Per DoW OIG (b)(6) (b)(7)(C) Per [redacted] scanned computers on the net all the time. However getting in to the systems doesn't happen all the time. They are able to get into web pages that use Microsoft Frontpage software. Per DoW OIG (b)(6) (b)(7)(C) Per [redacted] advised that many of the older exploits such as "stat-d" have been fixed. Per [redacted] advised that Per DoW OIG (b)(6) (b)(7)(C) computer was the one closest to the garage door but that Per [redacted] used the cable modem Internet hook up attached to Per DoW OIG (b)(6) (b)(7)(C) (nearest the garage entry into the house all the time.

Per [redacted] advised that Per DoW OIG (b)(6) (b)(7)(C) hacker name was Per [redacted] and that his was Per DoW OIG (b)(6) (b)(7)(C). Later in the interview Per [redacted] acknowledged that Per [redacted] was also known as Per DoW OIG (b)(6) (b)(7)(C). Per [redacted] advised that Per [redacted] had conducted several hacks of DOD web sites. While at Per DoW OIG (b)(6) (b)(7)(C) stated that Per [redacted] conversed with a hacker Per DoW OIG (b)(6) (b)(7)(C) during an IRC session. Per [redacted] told them that he had taken files and software from the Defense Information Systems Agency (DISA) computers. During the IRC with Per [redacted] he showed them screen shots of some Defense Information Systems Network (DISN) software that he, Per [redacted] had taken from a DISA computer. Later Per [redacted] saw the software on the Anti-on-line web site. Per [redacted] at first thought the DISN software was classified but then later heard that the DOD stated that it was not.

CLASSIFICATION:

FOR OFFICIAL USE ONLY**WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving agency without specific prior authorization of the Assistant Inspector General for Investigations.

[redacted] explained that he did not know all the members of the hacker group known as the Masters of Downloading (MOD). [redacted] knew that [redacted] was a member and that [redacted] used each other as [redacted] was knowledgeable in Windows NT and [redacted] was knowledgeable in the UNIX operating system. They did not like each other but they would discuss hacking information. [redacted] was a member of the MOD and another hacker named [redacted] was also a member. [redacted] and he is also a member of the group MilWorm that did the Nuclear software hack in the Indian Computers during the recent Indian nuclear weapons testing.

[redacted] identified other MilWorm members as [redacted] (unknown location) and [redacted]. [redacted] heard that the NSA (National Security Agency) monitored the Milworm's nuclear software hack in real-time. [redacted] stated that the hack was accomplished using send mail exploits because the Indian computers are not as up to date as US computers and they are easily hacked with older known exploits. [redacted] advised that the MilWorm group routed through several US Government systems to accomplish the hack to the Indian computer system.

When first asked he denied ever hacking into any military DOD computer or other commercial web site. He claims he never got into a government system. [redacted] has hacked several web sites and left his mark of his hacker group known as the NOID. [redacted] hacked the Pentagon web page by changing the index HTML for the web page using Frontpage software by Microsoft. [redacted] did not actually see him do the hack but saw a copy of the hacked web page on a Swedish web site known as flashback.se. [redacted] showed him the page on the Swedish site and told him he had done it. SA [redacted] showed [redacted] a printed copy of the altered Pentagon web page and [redacted] stated that it was the same that [redacted] claimed he had altered. This document is attached to and made a part of this report (see attachment one). [redacted] identified the second page of the document as [redacted] hacker symbol.

SA [redacted] allowed [redacted] to review two more hacked web site pages. The first was an Army Information Systems Software Headquarters web page. The subject document had a header that spelled out NOID. [redacted] advised that this was also done by [redacted] and that anything that had the NOID or [redacted] on it was done by [redacted]. This document is attached to and made a part of this report (see attachment two). The second was a hacked web page from a Navy site which is attached to and made a part of this report (see attachment three). [redacted] advised that if it had NOID on it that it was [redacted] work. Another hacked web page titled "The Truth is a Virus" and www.legislate.com was shown to [redacted] and he identified it as [redacted] work. The www.legislate.com web page is attached to and made a part of this report (see attachment four). In the above mentioned hacked pages [redacted] claimed he was not there when the hacks occurred. [redacted] claimed that the NOID is over now. [redacted] added that [redacted] had ran away from home before and that some of the hacks occurred while [redacted] was living away from home. [redacted] claimed the only other NOID member he knew was [redacted]. [redacted] IRC Internet Protocol address ended in (.ca) which indicated Canada. He thought [redacted] may have helped [redacted] in the past as he was good with UNIX. [redacted] did not know what exploits or techniques were used by [redacted] to enter and change the .mil web site pages.

[redacted] spoke to [redacted] who is into UNIX and asked him for a filtering command and recalled having discussions with [redacted]. About four (4) weeks ago [redacted] gave [redacted] a user account and ID to use a shell account. Additionally [redacted] was given a UNIX shell account in Canada.

CLASSIFICATION:

FOR OFFICIAL USE ONLY

WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving agency without specific prior authorization of the Assistant Inspector General for Investigations.

from someone else (NFI) [Per DoW] advised that the PHF exploit is used to hack most systems. Getting a UNIX shell account is the only way to do a PHF hack.

[Per DoW] explained that it was easy to identify most of the Military and Army sites. In UNIX while on the net you just enter the command host -l and it will identify all the Army sites. He then commented that commercial web sites are easy to get into but when asked said he did not know any specific sites.

[Per DoW] explained that most of his and [Per DoW]'s activities were scanning networks using Wsping Pro for Windows. He explained that you can enter IP addresses and subnet address and that it will identify all class C and class D subnets. [Per DoW] also had a program that was two days old called Mscan which was UNIX based scanner by JS Bach of Oakland. This program will identify computers that are susceptible to the "STAT-D", and "PHF" exploits. It is a private release and you need to know someone to get a copy. [Per DoW] advised that he and [Per DoW] ran it against the University of California's Santa Barbara (UCSB) computer network. Mscan also identifies what ports are open on the computer being scanned. [Per DoW] stated that he and [Per DoW] kept up on software and operating system exploits by visiting and downloading the latest information from the "rootshell.com" web site.

[Per DoW] explained that they would scan the sites first and then try remote exploits against the system. Again he claimed that he had not actually hacked any sites. SA [Per DoW] then showed [Per DoW] a copy of an article posted to the Anti-on-line Web site (ANTIONLINE.COM). The article stated that the Navy was under fire. This document is attached to and made a part of this report as (attachment five). The article explained that the Navy had been hit with another famous free [Per DoW] protest and listed the following systems as being affected.

http://jax3b2.navy.mil
http://www.icas.spear.navy.mil
http://www.nctsjax.navy.mil
http://lej-www.med.navy.mil
http://www.nhttp.med.navy.mil
http://www.nmclanna.nadn.navy.mil

[Per DoW] admitted that he had done all the above sites. [Per DoW] advised that he placed no malicious code on the computers. He claimed he just altered the HTML index for the web site using Microsoft's Frontpage software and then uploaded the new page to the sight. [Per DoW] claimed that no exploit was needed only Frontpage. He just changed the HTML index and added the Free [Per DoW] and then placed it back on the sites. All he had to do was find a computer that ran Windows NT and used Front page and he could change the look of the page. He claimed he did the hacks on last Friday or Saturday (June 26, or 27 1998) night using his lap top computer and he did it from his home. He was alone and stated "I just did it for the hell of it." [Per DoW] stated that he thought [Per DoW] needs a trial. [Per DoW] acknowledged that [Per DoW] hacked a super computer in San Diego, California. [Per DoW] advised that he [Per DoW] did not think he had done anything wrong and remarked "it's not my fault the government is stupid."

Shortly after the Navy.mil attacks, [Per DoW] had an IRC discussion with a hacker from Bulgaria known as [Per DoW] told [Per DoW] that he [Per DoW] had done the Navy.mil hacks and [Per DoW] then E-mailed

CLASSIFICATION:

FOR OFFICIAL USE ONLY

WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving agency without specific prior authorization of the Assistant Inspector General for Investigations.

the story to the Anti-on-line web site. Per [redacted] claimed that these were the only sites he had done.

Per [redacted] explained that he has a Linux box, a notebook computer and that he also used Per DoW [redacted] computer located in the living room for Internet access. Per [redacted] stated that he had just recently installed the Linux operating system software on his notebook. Per DoW [redacted] (b)(6) (b)(7)(C) agreed to voluntarily surrender the notebook computer to the reporting agents for analysis. There was also a Macintosh computer sitting on the dining table.

Per [redacted] advised that he had talked with Per [redacted] approximately three days ago. Per [redacted] advised he left Per DoW [redacted] because he thought he was going to get in trouble. Per [redacted] would not state the reasons he felt he was about to get in trouble. At first Per [redacted] stated that Per [redacted] did not tell him anything. However, a short time later Per [redacted] admitted that Per [redacted] had called him on Friday afternoon and told him that "he had been raided, they took all his stuff" (the computers) and then he told Per [redacted] to, "expect visitors and not to tell them anything." Per [redacted] did not know if Per [redacted] had told anyone else and that they only talked five or six minutes.

Per [redacted] and Per [redacted] don't like each other and they don't have discussions on IRC. Per [redacted] and Per [redacted] don't like each other but they have discussions concerning each others questions regarding operation systems. Per [redacted] said that Per [redacted] stole the DOD software and he called it DISN software. At the time Per [redacted] thought it was classified software.

Later some guy from India wanted to buy the software. The guy sent Per [redacted] some money but Per [redacted] advised that Per [redacted] was not actually going to give the guy the software. Per [redacted] advised that the guy wanted it for the source code as they don't have good hierarchical structure and data bases in India. Per [redacted] thought they wanted it so they could make a database like it. Per [redacted] told Per [redacted] that the guy was an idiot. He did not know how much money the guy sent but thought it might have been three hundred dollars (\$300). Per [redacted] drove Per DoW [redacted] to a Post Office in Irvine, CA to pick up the money. Per [redacted] told Per [redacted] that he would not give Per [redacted] the software. They talked to the guy on ICQ and Per [redacted] thought the guys name was Per [redacted]. At first Per [redacted] stated that he talked with Per [redacted] once on IRC. However, Per [redacted] then stated that the last time he spoke with Per DoW [redacted] (b)(6) [redacted] cussed Per [redacted] out. Per [redacted] was asking too many personal questions, that he wanted the VB source code and he wanted to know the members of the MOD and MilWorm groups. Per [redacted] also wanted to do voice chat, but Per [redacted] does not have a fast enough Modem. Per DoW [redacted] last IRC discussion with Per [redacted] occurred approximately one week ago. Per [redacted] advised that he did not maintain logs of his IRC or ICQ (similar to IRC) discussions. Per [redacted] related that he has been seeing Per [redacted] on line for the last four or five months.

Per [redacted] was the hacker that stole the software, and according to Per DoW [redacted] (b)(6) [redacted] had been questioned about it by the London police. Per [redacted] opined that Per [redacted] had gotten rid of the software. Per [redacted] is P years old and had bragged that he was going to rent or buy a four story firehouse in London. Per [redacted] was also in a hacker group known as Code O. Per [redacted] wanted to talk with Per [redacted] as he had questions regarding Windows NT. Per [redacted] advised that Per [redacted] codes in Visual Basic (VB) and that Per DoW [redacted] (b)(6) [redacted] wants to write a suite of security utilities. Per [redacted] wanted to work with Per [redacted] on the security utilities. Per [redacted] wrote the Corescan and Ogre programs. The Ogre program scans a remote system for security holes and tells if they are available. Per [redacted] is currently writing an update for the Ogre program. According to Per [redacted]

CLASSIFICATION:

FOR OFFICIAL USE ONLY

WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving agency without specific prior authorization of the Assistant Inspector General for Investigations.

Per [REDACTED] specializes in Windows NT and by using Frontpage software that comes with Windows, you can easily change or alter a web page. Per [REDACTED] advised that Per DoW [REDACTED] had discussions with Per [REDACTED] regarding the Per DoW [REDACTED] and Per DoW [REDACTED] (b)(6) (b)(7)(C) [REDACTED] that were busted for breaking into the DOD computer systems. Per [REDACTED] advised Per DoW [REDACTED] broke into a DOD UNIX system using the Stat-d exploit.

On at least two occasions two guys came buy Per DoW [REDACTED] (b) and they talked regarding Windows NT. They bought Pizza and coke and Per DoW [REDACTED] showed them Ogre. Per [REDACTED] thought the two were Windows security or system administrators somewhere. Their handles were Per DoW [REDACTED] (b)(6) Per DoW [REDACTED] (b)(6) were concerned that the two wanted to steal Per DoW [REDACTED] (b)(6) Ogre source code. They visited at the Per DoW [REDACTED] (b)(6) on at least two occasions, both times on Friday evenings. They both had very good jobs and made good money. Per DoW [REDACTED] (b)(6) originally met the two on line in IRC. Then a visit was set up to meet and to discuss Windows NT. Per [REDACTED] claimed that they did not do any hacking with the two individuals. Per [REDACTED] advised Per DoW [REDACTED] (b)(6) (b)(7)(C) [REDACTED]. The two gave Per DoW [REDACTED] (b)(6) a copy of Novell 4.1 with the manuals. Per [REDACTED] did not think that Per DoW [REDACTED] (b)(6) and Per [REDACTED] do anything illegal but one of them had Per DoW [REDACTED] (b)(6) (b)(7)(C) [REDACTED] on his computer.

Per [REDACTED] advised that he and Per [REDACTED] did not do Denial of Service (DOS) attacks as they were a lamer prank. Per [REDACTED] claimed he had no information regarding credit card misuse. Per [REDACTED] advised that he thought only lamers do it and you could get in trouble for it. Per [REDACTED] stated that Per DoW [REDACTED] (b)(6) [REDACTED]

Per [REDACTED] advised that Per DoW [REDACTED] (b)(6) (b) [REDACTED] and did have a telephone lineman's handset as well as a tone box. The last time Per [REDACTED] saw the items, they were in a black backpack owned by Per DoW [REDACTED] (b)(6) Per [REDACTED] never saw Per [REDACTED] use the set other than once while at the Per [REDACTED] residence. Per [REDACTED] hooked the line set up to the residence phone lines to show Per [REDACTED] how it worked. Per [REDACTED] advised that he saw the tone box but that in order for it to work you have to modify it.

Per [REDACTED] advised that both he and Per [REDACTED] worked for a Per DoW [REDACTED] (b)(6) (b) [REDACTED] located in Per [REDACTED] (b)(7)(C) [REDACTED] as follows:

Per DoW [REDACTED] (b)(6) (b)(7)(C) [REDACTED]

Per [REDACTED] advised that he had not called his work since he left Trabuco Canyon and that he was going to call and let them know he was gone. They worked five hours a day for Per DoW [REDACTED] (b)(6) (b) [REDACTED] advised that he Per DoW [REDACTED] (b)(6) (b)(7)(C) [REDACTED]

Per DoW [REDACTED] (b)(6) (b)(7)(C) [REDACTED]

Per [REDACTED] upon his return home which was unexpected told Per DoW [REDACTED] (b)(6) (b) [REDACTED] that Per DoW [REDACTED] (b)(6) (b) [REDACTED] were out of town. Per DoW [REDACTED] (b)(6) (b) [REDACTED] interjected that Per [REDACTED] had been acting extremely nervous since his return. Per [REDACTED] was advised that the agents did not feel he told us everything. He stated that he did not do

CLASSIFICATION:

FOR OFFICIAL USE ONLY

WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving agency without specific prior authorization of the Assistant Inspector General for Investigations.

anything wrong and had nothing else to say. Per [redacted] was asked if he had any questions for the agents and responded in the negative. Per [redacted] then stated that [redacted]

was advised that [redacted]

Per DoW OIG (b)(6) (b)(7)(C)

Per DoW OIG (b)(6) (b)(7)(C)

He was advised that [redacted]

Per DoW OIG (b)(6) (b)(7)(C)

Per DoW
OIG (b)

Per [redacted] provided Per DoW OIG (b)(6) address as follows:

Per DoW OIG (b)(6) (b)(7)(C)

Per DoW [redacted] provided her Phone as Per DoW OIG [redacted] work and Per DoW OIG [redacted] home. Per DoW [redacted] work number was provided as Per DoW OIG (b)(6) (b)(7)(C). The interview was ended and Per DoW [redacted] advised she would walk reporting agents out. After getting outside Per DoW OIG [redacted] advised that Per DoW OIG (b)(6) (b)(7)(C). In addition, she stated that the agents handled the interview very professionally and in a non-threatening manner. Per DoW OIG (b)(6) encouraged Per DoW [redacted] to discuss Per DoW OIG [redacted] responses to the agents and attempt to get him to tell all the facts. She acknowledged that he only admitted to what he was shown and that Per DoW OIG [redacted] (b)(6) (b)(7)(C)

Prepared by SA [redacted]

b6 Per FBI
b7C Per FBI

CLASSIFICATION:

FOR OFFICIAL USE ONLY

WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving agency without specific prior authorization of the Assistant Inspector General for Investigations.

TOTAL P.07